

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-326166

(43)Date of publication of application : 16.12.1997

(51)Int.Cl. G11B 20/10

G09C 1/00

H04L 9/08

(21)Application number : 08-144460 (71)Applicant : MITSUBISHI ELECTRIC
CORP

(22)Date of filing : 06.06.1996 (72)Inventor : SAKAI YASUYUKI
YAMAGISHI ATSUHIRO
TAKEDA EISAKU

(54) METHOD AND SYSTEM FOR PROTECTING COPYRIGHT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection method capable of protecting a right of an author.

SOLUTION: In a transmission side of digital information, the digital information is ciphered by a first ciphering key, and the first ciphering key is ciphered by a second ciphering key. Then, the ciphered digital information is added with the ciphered first ciphering key to be transmitted. Then, in the receiving side of the digital information, the ciphered first ciphering key is deciphered by the second

ciphering key, and the ciphered digital information is deciphered by the first ciphering key obtained by the result of the deciphering.

LEGAL STATUS

[Date of request for examination]	16.02.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	abandonment
[Date of final disposal for application]	18.01.2002
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]

[Claim 1] The step which enciphers said digital information with the 1st encryption key in the transmitting side of digital information, Have the step which enciphers said 1st encryption key with the 2nd encryption key, and the step which adds said 1st enciphered encryption key to said enciphered digital

information, and is transmitted to it, and it sets to the receiving side of said digital information. The protection-of-copyrights approach characterized by having the step which decodes said 1st enciphered encryption key using said 2nd encryption key, and the step which decodes said enciphered digital information using the 1st encryption key obtained as a result of this decode.

[Claim 2] The protection-of-copyrights approach according to claim 1 characterized by using the encryption key out of which the transmitting side of said digital information and the receiving side came, respectively, and which was beforehand held as said 2nd encryption key.

[Claim 3] The protection-of-copyrights approach according to claim 1 characterized by using the encryption key given as said 2nd encryption key by equipment different from the transmitting side of said digital information, and a receiving side.

[Claim 4] The copyright protection system equipped with the following elements.

(a) The sending set equipped with the following means.

(a1) A means to encipher digital information with the 1st encryption key;

(a2) A means to encipher said 1st encryption key with the 2nd encryption key;

(a3) A means to add said 1st enciphered encryption key to said enciphered digital information, and to transmit to it.

(b) The receiving set equipped with the following means.

(b1) A means to decode said 1st enciphered encryption key using said 2nd encryption key;

(b2) A means to decode said enciphered digital information using the 1st encryption key obtained as a result of decode.

[Claim 5] The copyright protection system according to claim 4 characterized by using the encryption key out of which the transmitting side of said digital information and the receiving side came, respectively, and which was beforehand held as said 2nd encryption key.

[Claim 6] The copyright protection system according to claim 4 characterized by using the encryption key given as said 2nd encryption key by equipment different

from the transmitting side of said digital information, and a receiving side.

[Claim 7] The copyright protection system equipped with the following elements.

(a) The 1st equipment equipped with the following elements.

(a1) Key information on this 1st equipment proper;

(a2) An encryption key generation means to generate a key;

(a3) An encryption means to use initial value as an encryption key, and to encipher said generated key and to encipher said key information by using this enciphered key as an encryption key;

(a4) A transmitting means to transmit said enciphered key and said enciphered key information to the 2nd equipment and 3rd equipment.

(b) The 2nd equipment equipped with the following elements.

(b1) A pseudo-random-number generation means to generate the pseudo-random number;

(b2) A decode means to decode said transmitted key using initial value, and to decode said enciphered key information using this decoded key;

(b3) An encryption means to use said generated pseudo-random number as an encryption key, and to encipher digital information and to encipher said generated pseudo-random number by using said decoded key information as an encryption key;

(b4) A transmitting means to transmit said enciphered digital information and said enciphered pseudo-random number to the 3rd equipment.

(c) The 3rd equipment equipped with the following elements.

(c1) A decode means to decode the key information transmitted by the transmitting means of said 1st equipment, to decode the pseudo-random number transmitted by the transmitting means of said 2nd equipment using this decoded key information, and to decode the digital information transmitted by the transmitting means of said 2nd equipment using this decoded pseudo-random number.

[Claim 8] The encryption key generation means of said 1st equipment is a copyright protection system according to claim 7 characterized by generating the

encryption key of a proper to a system.

[Claim 9] It is the copyright protection system according to claim 7 characterized by for the encryption key generation means of said 1st equipment to generate an encryption key using ID information which identifies said 2nd and 3rd equipment, and for the decode means of said 2nd equipment to decode said enciphered key information using the encryption key generated by said encryption key generation means.

[Claim 10] It is the copyright protection system according to claim 7 characterized by for the encryption key generation means of said 1st equipment to generate an encryption key using ID information which identifies said 1st, 2nd, and 3rd equipment, and for the decode means of said 2nd equipment to decode said enciphered key information using the encryption key generated by said encryption key generation means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention prevents the unjust duplicate of data and relates to the protection-of-copyrights approach and copyright protection system which can protect an author's access.

[0002]

[Description of the Prior Art] The equipment which reproduces the conventional DVD (Digital Video Disc) is explained.

[0003] Drawing 3 is the conventional optical disc system for reproducing DVD. drawing -- setting -- 301 -- for a CD-ROM decoder and 304, as for an error correction circuit and 306, a demodulator circuit and 305 are [a DVD regenerative apparatus and 302 / a disk and 303 / a multiplexer and 307] bus

interfaces. The DVD regenerative apparatus 301 is constituted so that DVD and the disk of both CD-ROMs can be played. Next, actuation is explained. The data by which reading appearance was carried out from the disk 302 are inputted into the CD-ROM decoder 303 and a demodulator circuit 304. In the CD-ROM decoder 303, the recovery in the case of CD-ROM and an error correction are performed. In a demodulator circuit 304, the signal by which reading appearance was carried out is recovered from a disk 302 to digital data. The data to which it restored are inputted into the error correction circuit 305, and perform the error correction of the data of a DVD format. In a multiplexer 306, data are chosen according to any of DVD and CD-ROM disks 302 are, and it outputs to the bus interface 307.

[0004]

[Problem(s) to be Solved by the Invention] The optical disc system which reproduces the conventional DVD did not process at all the digital data currently recorded on the disk, but it was reproducing it as it was recorded by it. Therefore, there was a trouble that it was easy to make the duplicate of the data currently recorded on the disk, and it was difficult to protect the access of the author of data.

[0005] The object of this invention is difficult to have been made in order to solve the starting trouble, and to make the duplicate of data, and it is to obtain the protection-of-copyrights approach and copyright protection system which can protect an author's access.

[0006]

[Means for Solving the Problem] The protection-of-copyrights approach concerning claim 1 of this invention is set to the transmitting side of digital information. The step which enciphers said digital information with the 1st encryption key, and the step which enciphers said 1st encryption key with the 2nd encryption key, Have the step which adds said 1st enciphered encryption key to said enciphered digital information, and is transmitted to it, and it sets to the receiving side of said digital information. It has the step which decodes said

1st enciphered encryption key using said 2nd encryption key, and the step which decodes said enciphered digital information using the 1st encryption key obtained as a result of this decode.

[0007] The encryption key out of which the transmitting side of said digital information and the receiving side came, respectively and which was beforehand held as said 2nd encryption key is used for the protection-of-copyrights approach concerning claim 2 of this invention.

[0008] The encryption key given as said 2nd encryption key by equipment with another transmitting side and receiving side of said digital information is used for the protection-of-copyrights approach concerning claim 3 of this invention.

[0009] The copyright protection system concerning claim 4 of this invention is equipped with the following elements.

(a) The sending set equipped with the following means.

(a1) A means to encipher digital information with the 1st encryption key;

(a2) A means to encipher said 1st encryption key with the 2nd encryption key;

(a3) A means to add said 1st enciphered encryption key to said enciphered digital information, and to transmit to it.

(b) The receiving set equipped with the following means.

(b1) A means to decode said 1st enciphered encryption key using said 2nd encryption key;

(b2) A means to decode said enciphered digital information using the 1st encryption key obtained as a result of decode.

[0010] The encryption key out of which the transmitting side of said digital information and the receiving side came, respectively and which was beforehand held as said 2nd encryption key is used for the copyright protection system concerning claim 5 of this invention.

[0011] The encryption key given as said 2nd encryption key by equipment with another transmitting side and receiving side of said digital information is used for the copyright protection system concerning claim 6 of this invention.

[0012] The copyright protection system concerning claim 7 of this invention is

equipped with the following elements.

(a) The 1st equipment equipped with the following elements.

(a1) Key information on this 1st equipment proper;

(a2) An encryption key generation means to generate a key;

(a3) An encryption means to use initial value as an encryption key, and to encipher said generated key and to encipher said key information by using this enciphered key as an encryption key;

(a4) A transmitting means to transmit said enciphered key and said enciphered key information to the 2nd equipment and 3rd equipment.

(b) The 2nd equipment equipped with the following elements.

(b1) A pseudo-random-number generation means to generate the pseudo-random number;

(b2) A decode means to decode said transmitted key using initial value, and to decode said enciphered key information using this decoded key;

(b3) An encryption means to use said generated pseudo-random number as an encryption key, and to encipher digital information and to encipher said generated pseudo-random number by using said decoded key information as an encryption key;

(b4) A transmitting means to transmit said enciphered digital information and said enciphered pseudo-random number to the 3rd equipment.

(c) The 3rd equipment equipped with the following elements.

(c1) A decode means to decode the key information transmitted by the transmitting means of said 1st equipment, to decode the pseudo-random number transmitted by the transmitting means of said 2nd equipment using this decoded key information, and to decode the digital information transmitted by the transmitting means of said 2nd equipment using this decoded pseudo-random number.

[0013] The copyright protection system concerning claim 8 of this invention equips a system with an encryption key generation means to generate the encryption key of a proper.

[0014] The copyright protection system concerning claim 9 of this invention is equipped with an encryption key generation means generate an encryption key using ID information which identifies said 2nd and 3rd equipment, and is equipped with a decode means decode said enciphered key information using the encryption key generated by said encryption key generation means, in said 2nd equipment in said 1st equipment.

[0015] The copyright protection system concerning claim 10 of this invention is equipped with an encryption key generation means generate an encryption key using ID information which identifies said 1st, 2nd, and 3rd equipment, and is equipped with a decode means decode said enciphered key information using the encryption key generated by said encryption key generation means, in said 2nd equipment in the 1st equipment.

[0016]

[Embodiment of the Invention]

The gestalt of 1 operation of the protection-of-copyrights approach by gestalt 1. this invention of operation is explained based on drawing 1 . Drawing 1 is the flow chart of the protection-of-copyrights approach by the gestalt of this operation.

[0017] Next, actuation is explained. First, the 2nd common encryption key is shared and held by the transmitting side and receiving side of digital information. The transmitting side of digital information prepares the 1st encryption key first. Next, digital information is enciphered using this 1st encryption key. Next, the 1st encryption key is enciphered with the 2nd encryption key currently shared and held. Next, the 1st enciphered encryption key is added to the enciphered digital information, and it transmits to it. The receiving side of digital information performs the next actuation. First, the 1st encryption key enciphered with the 2nd encryption key currently shared is decoded. Next, digital information is decoded using the 1st decoded encryption key.

[0018] By enciphering digital information as mentioned above and transmitting, an informational unjust duplicate can be prevented and an informational author's access can be protected.

[0019] With the gestalt 1 of the gestalt 2. aforementioned implementation of operation, although the 2nd encryption key was beforehand shared by the transmitting side and the receiving side, the 3rd person other than a transmitting side and a receiving side can also supply it.

[0020] The gestalt of 1 operation of the copyright protection system by gestalt 3. this invention of operation is explained based on drawing 2 . Drawing 2 is the block diagram of the copyright protection system by the gestalt of this operation. In drawing, 201 is the 1st equipment, for example, is pocket mold information record media, such as an IC card and a PC card. 202 is peculiar every equipment [the] 201, and, as for the key information on secrecy, 1st ID information that 203 identifies the 1st equipment 201, an encryption key generation means by which 204 generates an encryption key, 1st encryption means by which 205 enciphers the key information 202, and 206, the 1st decode means and 207 are the 1st interface. 208 is the 2nd equipment, for example, is DVD. For a pseudo-random-number generation means and 211, as for the 2nd decode means and 213, the 2nd encryption means and 212 are [209 / 2nd ID information and 210 / the 2nd interface and 214] digital information. The 2nd equipment 208 enciphers digital information 214, and is transmitted. 215 is the 3rd equipment which receives and decodes the digital information 214 which enciphered with the 2nd equipment 208 and was transmitted, for example, is a personal computer which a user uses. As for 216, 3rd ID information and 217 are initial value with which the 3rd decode means and 218 are stored in the 3rd interface, and 219 is stored in the 1st - the 3rd equipment, respectively.

[0021] Next, actuation is explained. First, the procedure in which three equipments, the 1st equipment 201, the 2nd equipment 208, and the 3rd equipment 215, share the key information 202 is explained. The key information 202 on a proper, the 1st ID information 203, and initial value 219 are beforehand written in the 1st equipment 201. The 2nd ID information 209 and initial value 219 are beforehand written in the 2nd equipment 208. The 3rd ID information 216 and initial value 219 are beforehand written in the 3rd equipment 215. Initial value

219 is a common value in the 1st equipment 201, 2nd equipment 208, and 3rd equipment 215. First, an encryption key is generated in the encryption key generation means 204 of the 1st equipment 201, initial value 219 is enciphered as an encryption key with the 1st encryption means 205, and the encryption key is transmitted to the 2nd equipment 208 and 3rd equipment 215 through the 1st interface 207. It is decoded with the 2nd equipment 208 and 3rd equipment 215, and the encryption key generated in the encryption key generation means 204 is a key of a proper, and is shared between three equipments by three equipments which constitute a system. Next, using this shared encryption key, the key information 202 is enciphered in the 1st encryption means 205, and it is transmitted to the 2nd equipment 208 and 3rd equipment 215 through the 1st interface 207. Next, in the 2nd decode means 212 and the 3rd decode means 217, the enciphered key information 202 is decoded and the key information 202 is shared by three equipments.

[0022] Next, the procedure of transmitting the digital information 214 of the 2nd equipment 208 to the 3rd equipment 215 is explained. First, the pseudo-random number is generated in the pseudo-random-number generation means 210, and digital information 214 is enciphered by using the generated pseudo-random number as an encryption key. The generated pseudo-random number is enciphered with the 2nd encryption means 211 by using key information 202 as an encryption key. The digital information 214 enciphered as the enciphered pseudo-random number is transmitted to the 3rd equipment 215 through the 2nd interface 213. With the 3rd equipment 215, the pseudo-random number enciphered first is decoded using the key information 202 currently shared. Next, the enciphered digital information 214 is decoded using the decoded pseudo-random number, and the original digital information 214 is acquired. Since it is enciphered when transmitting digital information, the copyright protection system of the gestalt of this operation can prevent the unjust duplicate of digital information, and can protect an author's access.

[0023] In the 2nd equipment 208 and 3rd equipment 215, although the shared

key information 202 was held, if it is made to hold only when transmitting digital information 214, and transmission is completed, when eliminating from the inside of equipment and starting the next transmission, it can share between the gestalt 3 of the gestalt 4. aforementioned implementation of operation again.

[0024] Although initial value 219 was used as the encryption key with the gestalt 3 of the gestalt 5. aforementioned implementation of operation when transmitting the key information 202 to the 2nd equipment 208 and 3rd equipment 215 First, transmit the 3rd ID information 216 which the 2nd ID information 209 which the 2nd equipment 208 holds, and the 3rd equipment 215 hold to the first equipment [1st] 201, and it sets to the 1st equipment 201. The key information 202 which only the 1st equipment 201 holds based on the 2nd ID information 209 and the 3rd ID information 216 which have been sent from the 1st ID information 203, 2nd equipment 208, and 3rd equipment 215 as a parameter of secrecy A new encryption key can be generated in the encryption key generation means 204, and this can also be used instead of initial value 219.

[0025] What is necessary is just to perform as follows the encryption key generated with the encryption key generation means 205 in order to encipher the key information 202 with the gestalt 3 of the gestalt 6. aforementioned implementation of operation, when either of these three equipments interchanges to another equipment although held with the 1st equipment 201, 2nd equipment 208, and 3rd equipment 215. First, the encryption key generation means 204 generates a new encryption key using the 1st ID information 203, the 2nd ID information 209, and the 3rd ID information 216. Next, initial value 219 is enciphered as an encryption key with the 1st encryption means 205, and the generated encryption key is transmitted to the 2nd equipment 208 and 3rd equipment 215. It decodes using initial value 219 and the new encryption key generated with the encryption key generation means 204 is shared by the 2nd equipment 208 and 3rd equipment 215.

[0026] DVD (Digital Video Disc), CD-ROM, etc. can also use the protection-of-copyrights approach of the gestalten 1-6 the gestalt 7. aforementioned

implementation operation, and a copyright protection system for the regenerative apparatus of a digital information record medium at large. Moreover, although the 1st equipment 201 was used as pocket mold information record media, such as an IC card and a PC card, it should just be the record medium which can hold the key information 202 in secrecy.

[0027]

[Effect of the Invention] As mentioned above, the protection-of-copyrights approach and copyright protection system by this invention can prevent the unjust duplicate of digital information, and are effective in the ability to protect an author's access.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing explaining the protection-of-copyrights approach of this invention.

[Drawing 2] It is the block diagram of the copyright protection system of this invention.

[Drawing 3] It is the block diagram of the conventional optical disc system.

[Description of Notations]

201 1st Equipment, 202 Key Information, 203 1st ID Information, 204 An encryption key generation means, 205 The 1st encryption means, 206 The 1st decode means, The 207 1st interface, 208 The 2nd equipment, 209 2nd ID information, 210 A pseudo-random-number generation means, 211 The 2nd encryption means, 212 The 2nd decode means, 213 The 2nd interface, 214 Digital information, 215 The 3rd equipment, 216 3rd ID information, 217 The 3rd decode means, 218 The 3rd interface, 219 Initial value.

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平9-326166

(43)公開日 平成9年(1997)12月16日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
		7259-5 J		6 3 0 A
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 D
				6 0 1 A
審査請求 未請求 請求項の数10 O L (全 7 頁)				

(21)出願番号 特願平8-144460

(22)出願日 平成8年(1996)6月6日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 酒井 康行

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 山岸 篤弘

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 竹田 栄作

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

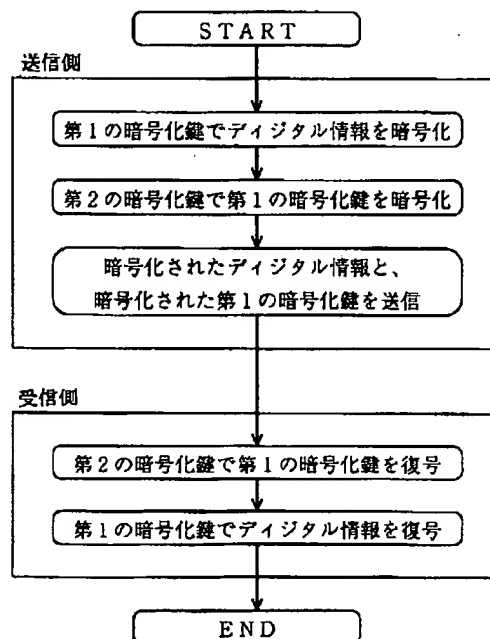
(74)代理人 弁理士 宮田 金雄 (外3名)

(54)【発明の名称】 著作権保護方法及び著作権保護システム

(57)【要約】

【課題】 著作権者の権利を保護できる著作権保護方法を得る。

【解決手段】 デジタル情報の送信側において、前記デジタル情報を第1の暗号化鍵で暗号化するステップと、第2の暗号化鍵で前記第1の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信するステップとを備え、前記デジタル情報の受信側において、前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号するステップと、この復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたものである。



【特許請求の範囲】

【請求項1】 デジタル情報の送信側において、第1の暗号化鍵で前記デジタル情報を暗号化するステップと、第2の暗号化鍵で前記第1の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信するステップとを備え、

前記デジタル情報の受信側において、前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号するステップと、この復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたことを特徴とする著作権保護方法。

【請求項2】 前記第2の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項1に記載の著作権保護方法。

【請求項3】 前記第2の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項1に記載の著作権保護方法。

【請求項4】 以下の要素を備えた著作権保護システム。

(a) 以下の手段を備えた送信装置。

(a 1) 第1の暗号化鍵でデジタル情報を暗号化する手段；

(a 2) 第2の暗号化鍵で前記第1の暗号化鍵を暗号化する手段；

(a 3) 前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信する手段。

(b) 以下の手段を備えた受信装置。

(b 1) 前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号する手段；

(b 2) 復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号する手段。

【請求項5】 前記第2の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項4に記載の著作権保護システム。

【請求項6】 前記第2の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項4に記載の著作権保護システム。

【請求項7】 以下の要素を備えた著作権保護システム。

(a) 以下の要素を備えた第1の装置。

(a 1) この第1の装置固有の鍵情報；

(a 2) 鍵を生成する暗号化鍵生成手段；

(a 3) 初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；

(a 4) 前記暗号化した鍵及び前記暗号化した鍵情報を第2の装置と第3の装置に送信する送信手段。

(b) 以下の要素を備えた第2の装置。

(b 1) 擬似乱数を生成する擬似乱数生成手段；

(b 2) 初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；

(b 3) 前記生成した擬似乱数を暗号化鍵としてデジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；

(b 4) 前記暗号化したデジタル情報及び前記暗号化した擬似乱数を第3の装置に送信する送信手段。

(c) 以下の要素を備えた第3の装置。

(c 1) 前記第1の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第2の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第2の装置の送信手段により送信されたデジタル情報を復号する復号手段。

【請求項8】 前記第1の装置の暗号化鍵生成手段は、システムに固有の暗号化鍵を生成することを特徴とする請求項7に記載の著作権保護システム。

【請求項9】 前記第1の装置の暗号化鍵生成手段は、前記第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成し、

前記第2の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項7に記載の著作権保護システム。

【請求項10】 前記第1の装置の暗号化鍵生成手段は、前記第1、第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成し、

前記第2の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項7に記載の著作権保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データの不正な複製を防ぎ、著作権者の権利を保護できる著作権保護方法及び著作権保護システムに関する。

【0002】

【従来の技術】 従来のDVD (Digital Video Disc) を再生する装置について説明する。

【0003】 図3は、DVDを再生するための従来の光ディスクシステムである。図において301はDVD再生装置、302はディスク、303はCD-ROMデコーダ、304は復調回路、305は誤り訂正回路、306はマルチプレクサ、307はバスインタフェースである。DVD再生装置301はDVDとCD-ROMの両方のディスクを再生できるように構成されている。次に

動作を説明する。ディスク 302 から読み出されたデータは、CD-ROM デコーダ 303 および復調回路 304 に入力される。CD-ROM デコーダ 303 では CD-ROM の場合の復調、誤り訂正が行われる。復調回路 304 ではディスク 302 から読み出された信号をデジタルデータに復調する。復調されたデータは、誤り訂正回路 305 に入力され、DVD フォーマットのデータの誤り訂正を行う。マルチプレクサ 306 では、ディスク 302 が DVD、CD-ROM のいずれであるかに応じてデータを選択し、バスインタフェース 307 に出力する。

【0004】

【発明が解決しようとする課題】従来の DVD を再生する光ディスクシステムは、ディスクに記録されているデジタルデータを何ら加工せず、記録されているままに再生していた。そのため、ディスクに記録されているデータの複製を作ることが容易であり、データの著作権者の権利を保護することが困難であるという問題点があった。

【0005】本発明の目的は、係る問題点を解決するためになされたもので、データの複製を作ることが困難で、著作権者の権利を保護することができる著作権保護方法及び著作権保護システムを得ることにある。

【0006】

【課題を解決するための手段】本発明の請求項 1 に係る著作権保護方法は、デジタル情報の送信側において、第 1 の暗号化鍵で前記デジタル情報を暗号化するステップと、第 2 の暗号化鍵で前記第 1 の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第 1 の暗号化鍵を付加して送信するステップとを備え、前記デジタル情報の受信側において、前記第 2 の暗号化鍵を用いて前記暗号化された第 1 の暗号化鍵を復号するステップと、この復号の結果得られた第 1 の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたものである。

【0007】本発明の請求項 2 に係る著作権保護方法は、前記第 2 の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【0008】本発明の請求項 3 に係る著作権保護方法は、前記第 2 の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【0009】本発明の請求項 4 に係る著作権保護システムは、以下の要素を備えたものである。

(a) 以下の手段を備えた送信装置。

(a 1) 第 1 の暗号化鍵でデジタル情報を暗号化する手段；

(a 2) 第 2 の暗号化鍵で前記第 1 の暗号化鍵を暗号化する手段；

(a 3) 前記暗号化されたデジタル情報に前記暗号化された第 1 の暗号化鍵を付加して送信する手段。

(b) 以下の手段を備えた受信装置。

(b 1) 前記第 2 の暗号化鍵を用いて前記暗号化された第 1 の暗号化鍵を復号する手段；

(b 2) 復号の結果得られた第 1 の暗号化鍵を用いて前記暗号化されたデジタル情報を復号する手段。

【0010】本発明の請求項 5 に係る著作権保護システムは、前記第 2 の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【0011】本発明の請求項 6 に係る著作権保護システムは、前記第 2 の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【0012】本発明の請求項 7 に係る著作権保護システムは、以下の要素を備えたものである。

(a) 以下の要素を備えた第 1 の装置。

(a 1) この第 1 の装置固有の鍵情報；

(a 2) 鍵を生成する暗号化鍵生成手段；

(a 3) 初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；

(a 4) 前記暗号化した鍵及び前記暗号化した鍵情報を第 2 の装置と第 3 の装置に送信する送信手段。

(b) 以下の要素を備えた第 2 の装置。

(b 1) 擬似乱数を生成する擬似乱数生成手段；

(b 2) 初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；

(b 3) 前記生成した擬似乱数を暗号化鍵としてデジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；

(b 4) 前記暗号化したデジタル情報及び前記暗号化した擬似乱数を第 3 の装置に送信する送信手段。

(c) 以下の要素を備えた第 3 の装置。

(c 1) 前記第 1 の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第 2 の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第 2 の装置の送信手段により送信されたデジタル情報を復号する復号手段。

【0013】本発明の請求項 8 に係る著作権保護システムは、システムに固有の暗号化鍵を生成する暗号化鍵生成手段を備えたものである。

【0014】本発明の請求項 9 に係る著作権保護システムは、前記第 1 の装置において、前記第 2 及び第 3 の装置を識別する ID 情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第 2 の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものであ

る。

【0015】本発明の請求項10に係る著作権保護システムは、第1の装置において、前記第1、第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第2の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものである。

【0016】

【発明の実施の形態】

実施の形態1. 本発明による著作権保護方法の一実施の形態を図1に基づいて説明する。図1は、本実施の形態による著作権保護方法のフローチャートである。

【0017】次に動作を説明する。まず、デジタル情報の送信側と受信側とで、共通の第2の暗号化鍵を共有し、保持しておく。デジタル情報の送信側は、まず第1の暗号化鍵を用意する。次にこの第1の暗号化鍵を用いてデジタル情報を暗号化する。次に、共有し保持されている第2の暗号化鍵で第1の暗号化鍵を暗号化する。次に、暗号化されたデジタル情報に、暗号化された第1の暗号化鍵を付加して送信する。デジタル情報の受信側は、次の動作を行う。まず、共有されている第2の暗号化鍵で暗号化された第1の暗号化鍵を復号する。次に、復号された第1の暗号化鍵を用いて、デジタル情報を復号する。

【0018】以上のようにデジタル情報を暗号化して送信することにより、情報の不正な複製を防ぐことができ、情報の著作権者の権利を保護することができる。

【0019】実施の形態2. 前記実施の形態1では、第2の暗号化鍵はあらかじめ送信側と受信側とで共有されていたが、送信側、受信側以外の第3者が供給することもできる。

【0020】実施の形態3. 本発明による著作権保護システムの一実施の形態を、図2に基づいて説明する。図2は、本実施の形態による著作権保護システムの構成図である。図において、201は第1の装置であり、例えばICカードおよびPCカードなどの携帯型情報記録媒体である。202は第1の装置201毎に固有でかつ秘密の鍵情報、203は第1の装置201を識別する第1のID情報、204は暗号化鍵を生成する暗号化鍵生成手段、205は鍵情報202を暗号化する第1の暗号化手段、206は第1の復号手段、207は第1のインタフェースである。208は第2の装置であり、例えばDVDである。209は第2のID情報、210は擬似乱数生成手段、211は第2の暗号化手段、212は第2の復号手段、213は第2のインタフェース、214はデジタル情報である。第2の装置208は、デジタル情報214を暗号化して送信する。215は第2の装置208により暗号化して送信されたデジタル情報214を受信して復号する第3の装置であり、例えばユー

ザが使用するパソコンである。216は第3のID情報、217は第3の復号手段、218は第3のインタフェース、219は第1～第3の装置にそれぞれ格納されている初期値である。

【0021】次に動作を説明する。まず、鍵情報202を、第1の装置201、第2の装置208及び第3の装置215の3つの装置で共有する手順を説明する。第1の装置201にはあらかじめ、固有の鍵情報202、第1のID情報203及び初期値219が書き込まれている。第2の装置208にはあらかじめ、第2のID情報209及び初期値219が書き込まれている。第3の装置215にはあらかじめ、第3のID情報216及び初期値219が書き込まれている。初期値219は、第1の装置201、第2の装置208及び第3の装置215において共通の値である。まず、第1の装置201の暗号化鍵生成手段204において暗号化鍵を生成し、その暗号化鍵は、第1の暗号化手段205により初期値219を暗号化鍵として暗号化され、第1のインタフェース207を介して第2の装置208及び第3の装置215に送信される。第2の装置208及び第3の装置215でそれが復号され、暗号化鍵生成手段204において生成された暗号化鍵は、システムを構成する3つの装置に固有の鍵であり、3つの装置で共有される。次に、この共有された暗号化鍵を用いて、第1の暗号化手段205において鍵情報202を暗号化し、第1のインタフェース207を介して第2の装置208及び第3の装置215に送信される。次に、第2の復号手段212及び第3の復号手段217において、暗号化された鍵情報202は復号され、鍵情報202は、3つの装置で共有される。

【0022】次に、第2の装置208のデジタル情報214を、第3の装置215に送信する手順を説明する。まず、擬似乱数生成手段210において擬似乱数を生成し、生成された擬似乱数を暗号化鍵としてデジタル情報214を暗号化する。生成された擬似乱数は、鍵情報202を暗号化鍵として第2の暗号化手段211により暗号化する。暗号化された擬似乱数と、暗号化されたデジタル情報214を、第2のインタフェース213を介して第3の装置215に送信する。第3の装置215では、共有されている鍵情報202を用いて、まず暗号化された擬似乱数を復号する。次に、復号された擬似乱数を用いて、暗号化されたデジタル情報214を復号し、元のデジタル情報214を得る。本実施の形態の著作権保護システムは、デジタル情報を送信するとき、暗号化されているので、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる。

【0023】実施の形態4. 前記実施の形態3では、第2の装置208及び第3の装置215において、共有の鍵情報202を保持していたが、デジタル情報214

を送信するときのみ保持するようにし、送信が終了したら装置内から消去し、次の送信を開始するときに、再び共有するようにすることもできる。

【0024】実施の形態5。前記実施の形態3では、鍵情報202を第2の装置208及び第3の装置215に送信するとき、初期値219を暗号化鍵としていたが、まず、最初の第1の装置201に対し、第2の装置208の保持する第2のID情報209および第3の装置215の保持する第3のID情報216を送信し、第1の装置201において、第1のID情報203と第2の装置208及び第3の装置215から送られてきた第2のID情報209及び第3のID情報216をもとに第1の装置201のみが保有している鍵情報202を秘密のパラメータとして新たな暗号化鍵を暗号化鍵生成手段204において生成し、これを初期値219の代わりに用いることもできる。

【0025】実施の形態6。前記実施の形態3では、鍵情報202を暗号化するために暗号化鍵生成手段205で生成した暗号化鍵は、第1の装置201、第2の装置208及び第3の装置215で保持されていたが、これら3つの装置のいずれかが、別の装置に入れ替わった場合は、次のようにすればよい。まず、第1のID情報203、第2のID情報209及び第3のID情報216を用いて、暗号化鍵生成手段204で新たな暗号化鍵を生成する。次に、生成された暗号化鍵を、第1の暗号化手段205で初期値219を暗号化鍵として暗号化し、第2の装置208及び第3の装置215に送信する。第2の装置208及び第3の装置215では初期値219を用いて復号し、暗号化鍵生成手段204で生成された新たな暗号化鍵は共有される。

【0026】実施の形態7。前記実施の形態1～6の著作権保護方法及び著作権保護システムは、DVD(Digital Video Disc)、CD-ROMなど、デジタル情報記録媒体全般の再生装置に用いることもできる。また、第1の装置201は、ICカードおよびPCカードなどの携帯型情報記録媒体としたが、鍵情報202を秘密に保持できる記録媒体であれば良い。

【0027】

【発明の効果】以上のように、本発明による著作権保護方法及び著作権保護システムは、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる効果がある。

【図面の簡単な説明】

【図1】 本発明の著作権保護方法を説明する図である。

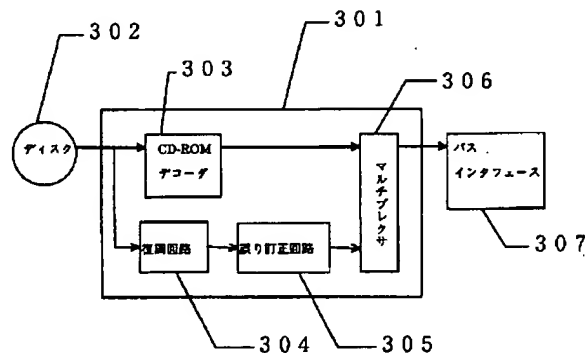
【図2】 本発明の著作権保護システムの構成図である。

【図3】 従来の光ディスクシステムの構成図である。

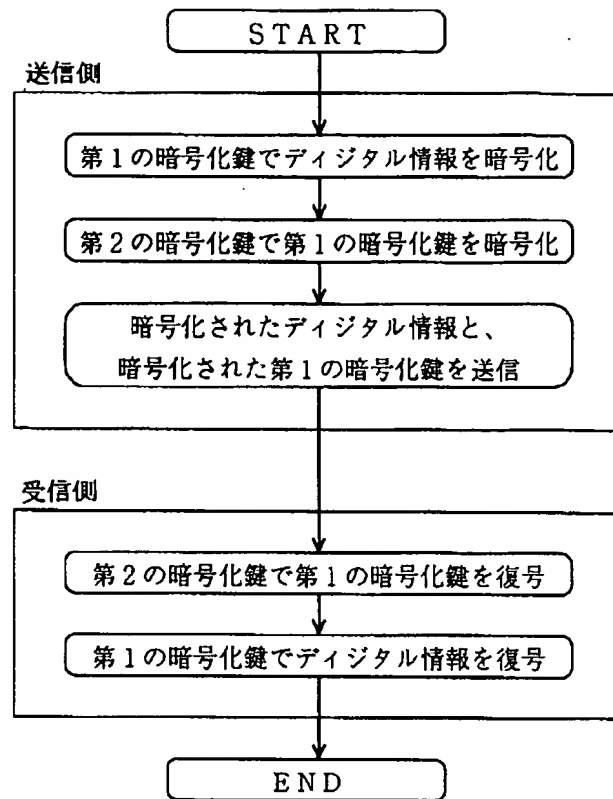
【符号の説明】

201 第1の装置、202 鍵情報、203 第1のID情報、204 暗号化鍵生成手段、205 第1の暗号化手段、206 第1の復号手段、207 第1のインタフェース、208 第2の装置、209 第2のID情報、210 擬似乱数生成手段、211 第2の暗号化手段、212 第2の復号手段、213 第2のインタフェース、214 デジタル情報、215 第3の装置、216 第3のID情報、217 第3の復号手段、218 第3のインタフェース、219 初期値。

【図3】



【図1】



【図2】

